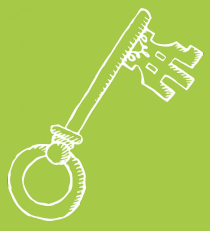

Are Attacks Faster than Brute-Force?

Advisor: **Christoph Dobraunig**

Motivation

In cryptanalysis, we research the security of cryptographic algorithms. The ultimate goal is typically to extract the secret key used by some entity. Naturally, such a key recovery attack's effectiveness is determined by comparing it to an exhaustive search for the secret key.

Recently, new attacks on round-reduce variants of Rasta have been proposed. Rasta is the current record holder in terms of minimizing the ANDdepth and usage of ANDs per encrypted bit. Your task in this project is to implement the proposed attacks and do experiments to compare them with a brute-force key search.

Goals and Tasks

- Get familiar with Rasta and the attack
- Create a faster version of the reference implementation
- Implement the brute-force key search and the attack
- Compare the running times of the brute-force key search and the attack

Literature

- C. Dobraunig et al.
  Framework for faster key search using related-key higher-order differential properties: applications to Agrasta
  IET Inf. Secur. 2020
  https://doi.org/10.1049/iet-ifs.2019.0326
- C. Dobraunig et al.
  Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit
  CRYPTO 2018

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

☑ **Bachelor Project**
Project code and documentation

☑ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Knowledge of C/C++
- Interest in cryptography

Advisor / Contact

christoph.dobraunig@iaik.tugraz.at